



3

35.C15052

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	:	Examiner: Not Assigned
MITSURU MAEDA	)	
	:	Group Art Unit: 2132
Application No.: 09/761,721	)	
	:	
Filed: January 18, 2001	)	
	:	
For: INFORMATION PROCESSING	)	May 2, 2001
APPARATUS AND METHOD	:	

Commissioner for Patents  
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicant hereby claims priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Application:

JAPAN

2000-012965

January 21, 2000

A certified copy of the priority document is enclosed.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our address given below.

Respectfully submitted,



Attorney for Applicant  
Brian L. Klock  
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200

BLK/dc



本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

09/761,721  
Mitsuru Maeda  
January 18, 2001

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

2000年 1月21日

出願番号  
Application Number:

特願2000-012965

出願人  
Applicant(s):

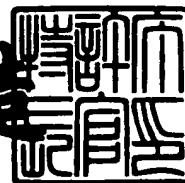
キヤノン株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 2月 9日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2001-3006275

【書類名】 特許願

【整理番号】 4144147

【提出日】 平成12年 1月21日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 H04L 9/00

【発明の名称】 画像処理装置及びその方法並びに記憶媒体

【請求項の数】 42

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 前田 充

【特許出願人】

【識別番号】 000001007

【住所又は居所】 東京都大田区下丸子3丁目30番2号

【氏名又は名称】 キャノン株式会社

【代表者】 御手洗 富士夫

【電話番号】 03-3758-2111

【代理人】

【識別番号】 100090538

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【弁理士】

【氏名又は名称】 西山 恵三

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100096965

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会  
社内

【弁理士】

【氏名又は名称】 内尾 裕一

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100110009

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
社内

【弁理士】

【氏名又は名称】 青木 康

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100069877

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
社内

【弁理士】

【氏名又は名称】 丸島 儀一

【電話番号】 03-3758-2111

【手数料の表示】

【予納台帳番号】 011224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9908388

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像処理装置及びその方法並びに記憶媒体

【特許請求の範囲】

【請求項 1】 画像データを入力する入力手段と、  
前記画像データを保護するためのセキュリティデータを生成する生成手段と、  
前記画像データを符号化し、符号化データを生成する符号化手段と、  
前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される所定符号を抽出する抽出手段と、  
前記所定符号に前記セキュリティデータを重畳する重畳手段と、  
前記セキュリティが設定された区間において前記所定符号を除いた前記符号化データにスクランブルを施すスクランブル手段と、  
前記重畳手段によって処理された所定符号と前記スクランブル手段によって処理された符号化データとを出力する出力手段とを有することを特徴とする画像処理装置。

【請求項 2】 前記セキュリティデータは前記スクランブル手段に使用されるキー情報を含むことを特徴とする請求項 1 に記載の画像処理装置。

【請求項 3】 前記セキュリティデータは認証のための情報を含むことを特徴とする請求項 1 又は 2 に記載の画像処理装置。

【請求項 4】 前記符号化手段は MPEG-4 のビットストリームを生成することを特徴とする請求項 1 ～ 3 のいずれか 1 項に記載の画像処理装置。

【請求項 5】 前記セキュリティに関する情報を示す IPMP データを生成する IPMP 符号化手段を有し、前記出力手段は前記 IPMP 符号化手段によって生成された IPMP データを出力することを特徴とする請求項 4 に記載の画像処理装置。

【請求項 6】 前記セキュリティデータを暗号化する暗号化手段を有し、前記重畳手段は前記暗号化手段によって暗号化されたセキュリティデータを重畳することを特徴とする請求項 1 ～ 5 のいずれか 1 項に記載の画像処理装置。

【請求項 7】 前記抽出手段によって抽出される符号はスタートコードであることを特徴とする請求項 1 ～ 6 のいずれか 1 項に記載の画像処理装置。

【請求項 8】 画像符号化データから一意に決定される所定符号にセキュリ

データが適応的に重畳され、前記所定符号を除いた画像符号化データに前記セキュリティデータに応じて適応的にスクランブル処理されている符号化データを入力する入力手段と、

前記符号化データから前記所定符号が存在する位置にある符号を抽出する符号抽出手段と、

前記抽出された符号からセキュリティデータを検出する検出手段と、

前記検出手段の検出結果に応じて前記符号化データをデスクランブル処理するデスクランブル手段と、

前記デスクランブル手段によってデスクランブル処理された画像符号化データを復号化する復号化手段とを有することを特徴とする画像処理装置。

【請求項 9】 前記セキュリティデータには認証判定のために認証データが含まれており、前記認証データに応じて認証判定を行なう認証手段を有することを特徴とする請求項 8 に記載の画像処理装置。

【請求項 10】 前記デスクランブル手段は前記認証手段の判定結果に応じてスクランブル処理された符号化データをデスクランブルすることを特徴とする請求項 8 に記載の画像処理装置。

【請求項 11】 前記セキュリティデータは暗号化されており、前記暗号化されたセキュリティデータを解読する解読手段を有することを特徴とする請求項 8 ～ 10 のいずれか 1 項に記載の画像処理装置。

【請求項 12】 前記画像符号化データは MPEG-4 のビットストリームデータであることを特徴とする請求項 8 に記載の画像処理装置。

【請求項 13】 前記入力手段はセキュリティに関する情報を示す IPMP データを入力することを特徴とする請求項 12 に記載の画像処理装置。

【請求項 14】 前記 IPMP データには認証判定のために認証データが含まれており、前記認証データに応じて認証判定を行なう認証手段を有することを特徴とする請求項 13 に記載の画像処理装置。

【請求項 15】 前記デスクランブル手段は前記認証手段の判定結果に応じてスクランブル処理された符号化データをデスクランブルすることを特徴とする請求項 14 に記載の画像処理装置。

【請求項 16】 前記セキュリティデータは暗号化されており、前記暗号化されたセキュリティデータを前記認証手段の判定結果に応じて解読する解読手段を有することを特徴とする請求項 14 又は 15 に記載の画像処理装置。

【請求項 17】 前記所定符号とはスタートコードであることを特徴とする請求項 8 ～ 16 のいずれか 1 項に記載の画像処理装置。

【請求項 18】 画像データを入力する入力工程と、  
前記画像データを保護するためのセキュリティデータを生成する生成工程と、  
前記画像データを符号化し、符号化データを生成する符号化工程と、  
前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される所定符号を抽出する抽出工程と、  
前記所定符号に前記セキュリティデータを重畳する重畳工程と、  
前記セキュリティが設定された区間において前記所定符号を除いた前記符号化データにスクランブルを施すスクランブル工程と、  
前記重畳処理された所定符号と前記スクランブル処理された符号化データとを出力する出力工程とを有することを特徴とする画像処理方法。

【請求項 19】 前記セキュリティデータは前記スクランブル工程に使用されるキー情報を含むことを特徴とする請求項 18 に記載の画像処理方法。

【請求項 20】 前記セキュリティデータは認証のための情報を含むことを特徴とする請求項 18 又は 19 に記載の画像処理方法。

【請求項 21】 前記符号化工程は MPEG-4 のビットストリームを生成することを特徴とする請求項 18 ～ 20 のいずれか 1 項に記載の画像処理方法。

【請求項 22】 前記セキュリティに関する情報を示す IPMP データを生成する IPMP 符号化工程を有し、前記出力工程は前記 IPMP 符号化工程によって生成された IPMP データを出力することを特徴とする請求項 21 に記載の画像処理方法。

【請求項 23】 前記セキュリティデータを暗号化する暗号化工程を有し、前記重畳工程は前記暗号化工程によって暗号化されたセキュリティデータを重畳することを特徴とする請求項 18 ～ 22 のいずれか 1 項に記載の画像処理方法。

【請求項 24】 前記抽出工程によって抽出される符号はスタートコードであることを特徴とする請求項 18 ～ 23 のいずれか 1 項に記載の画像処理方法。



【請求項 2 5】 画像符号化データから一意に決定される所定符号にセキュリティデータが適応的に重畳され、前記所定符号を除いた画像符号化データに前記セキュリティデータに応じて適応的にスクランブル処理されている符号化データを入力する入力工程と、

前記符号化データから前記所定符号が存在する位置にある符号を抽出する符号抽出工程と、

前記抽出された符号からセキュリティデータを検出する検出工程と、

前記検出工程の検出結果に応じて前記符号化データをデスクランブル処理するデスクランブル工程と、

前記デスクランブル処理された画像符号化データを復号化する復号化工程とを有することを特徴とする画像処理方法。

【請求項 2 6】 前記セキュリティデータには認証判定のために認証データが含まれており、前記認証データに応じて認証判定を行なう認証工程を有することを特徴とする請求項 2 5 に記載の画像処理方法。

【請求項 2 7】 前記デスクランブル工程は前記認証工程の判定結果に応じてスクランブル処理された符号化データをデスクランブルすることを特徴とする請求項 2 6 に記載の画像処理方法。

【請求項 2 8】 前記セキュリティデータは暗号化されており、前記暗号化されたセキュリティデータを解読する解読工程を有することを特徴とする請求項 2 5 ～ 2 7 のいずれか 1 項に記載の画像処理方法。

【請求項 2 9】 前記画像符号化データは MPEG-4 のビットストリームデータであることを特徴とする請求項 2 5 に記載の画像処理方法。

【請求項 3 0】 前記入力工程はセキュリティに関する情報を示す IPMP データを入力することを特徴とする請求項 2 9 に記載の画像処理方法。

【請求項 3 1】 前記 IPMP データには認証判定のために認証データが含まれており、前記認証データに応じて認証判定を行なう認証工程を有することを特徴とする請求項 3 0 に記載の画像処理方法。

【請求項 3 2】 前記デスクランブル工程は前記認証工程の判定結果に応じてスクランブル処理された符号化データをデスクランブルすることを特徴とする

請求項 3 1 に記載の画像処理方法。

【請求項 3 3】 前記セキュリティデータは暗号化されており、前記暗号化されたセキュリティデータを前記認証工程の判定結果に応じて解読する解読工程を有することを特徴とする請求項 3 1 又は 3 2 に記載の画像処理方法。

【請求項 3 4】 前記所定符号とはスタートコードであることを特徴とする請求項 2 5 ～ 3 3 のいずれか 1 項に記載の画像処理方法。

【請求項 3 5】 階層構造を形成する画像符号化データを入力する入力工程と、

前記画像符号化データから所定層の先頭を示す所定コードを抽出する抽出工程と、

前記抽出工程によって抽出された所定コードに画像保護のためのセキュリティデータを重畳する重畳工程とを有することを特徴とする画像処理方法。

【請求項 3 6】 前記セキュリティデータに応じて前記画像符号化データに暗号化を行なう暗号化工程とを有することを特徴とする請求項 3 5 に記載の画像処理方法。

【請求項 3 7】 階層構造を形成する画像符号化データに対して、所定階層の先頭を示す所定コードにセキュリティデータを重畳した符号化データを入力する入力工程と、

前記符号化データから前記所定コードが存在する位置にある符号を抽出する抽出工程と、

前記抽出された符号から前記セキュリティデータを検出する検出工程と、

前記検出工程の検出結果に応じて前記符号化データを復号化する復号化工程とを有することを特徴とする画像処理方法。

【請求項 3 8】 前記符号化データは暗号化されており、前記復号化工程には前記暗号化を解読する工程が含まれていることを特徴とする請求項 3 7 に記載の画像処理方法。

【請求項 3 9】 請求項 1 8 ～ 2 4 のいずれか 1 項に記載の画像処理方法を実行する制御プログラムを記憶したコンピュータにより読取り可能な記憶媒体。

【請求項 4 0】 請求項 2 5 ～ 3 4 のいずれか 1 項に記載の画像処理方法を

実行する制御プログラムを記憶したコンピュータにより読取り可能な記憶媒体。

【請求項 4 1】 請求項 3 5 又は 3 6 に記載の画像処理方法を実行する制御プログラムを記憶したコンピュータにより読取り可能な記憶媒体。

【請求項 4 2】 請求項 3 7 又は 3 8 に記載の画像処理方法を実行する制御プログラムを記憶したコンピュータにより読取り可能な記憶媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、画像処理装置及びその方法並ぶにその画像処理プログラムが記録されたコンピュータにより読取り可能な記憶媒体に関し、特に画像の著作権等の保護を行うための画像処理に関するものである。

【 0 0 0 2 】

【従来の技術】

従来、動画像の符号化方式として、フレーム内符号化方式である Motion JPEG や Digital Video 等の符号化方式や、フレーム間予測符号化を用いた H. 2 6 1、H. 2 6 3、MPEG-1、MPEG-2 等の符号化方式が知られている。これらの符号化方式は I S O (International Organization for Standardization: 国際標準化機構) や I T U (International Telecommunication Union: 国際電気通信連合) によって国際標準化されている。前者の符号化方式はフレーム単位で独立に符号を行うもので、フレームの管理がしやすいため、動画像の編集や特殊再生が必要な装置に最適である。また、後者の符号化方式はフレーム間予測を用いるため、符号化効率が高いという特徴を持っている。

【 0 0 0 3 】

さらにコンピュータ・放送・通信など多くの領域で利用できる、汎用的な次世代マルチメディア符号化規格として MPEG-4 の国際標準化作業が進められている。

【 0 0 0 4 】

また、上述したようなデジタル符号化規格の普及に伴い、コンテンツ業界からは著作権保護の問題が強く提起されるようになってきた。即ち、著作権が保護

されることが十分に保証されていない規格に対しては、安心して優良なコンテンツを提供することができない、という問題が生じている。

#### 【0005】

このため、MPEG-4 ではその標準の中で著作権の保護を行うようにIPMP (Intellectual Property Management & Protection)の機能を盛り込むべくパート1であるSystems (ISO 14496-1) にデータが記載できるようになった。詳細はISO 14496-1を参照されたい。

#### 【0006】

図11にMPEG-4の符号化データの構成例を示す。

#### 【0007】

図11において、1010はBIFS符号化データであり、パート1に記載されているオブジェクトの合成方法や各オブジェクトの同期等の情報が符号化されたものである。1011はIPMP符号化データであり、各ビットストリームのセキュリティに関する情報が記載されている。1012は動画像の画像データの符号化結果であるビデオ符号化データである。1013は動画像に付随するオーディオデータの符号化結果であるオーディオ符号化データである。

#### 【0008】

IPMP符号化データ1011に記載されている情報の例を図12に示す。

#### 【0009】

まず、セキュリティが設定された符号化データを示す情報が含まれている。図12ではビデオ符号化データ1012である。続いてこの符号化データの復号を許可できるかどうかを判定するための認証データが入っている。図12では「no nac」が認証データである。一般にこのデータは暗号化されている。本例では認証データ「canon」を逆転させた状態で暗号化されていることを示している。

#### 【0010】

さらに、ビデオに対してはセキュリティをシーケンスの一部に施すためにその保護するフレームの番号とそのフレームのデータがスクランブルによって暗号化されている場合には解読のためのキーを暗号化した情報が記載されている。図12ではビデオ符号化データの中でフレーム番号1から100までが解読キー「key」

で、フレーム番号1000から1260までを解読キー「maeda」でデスクランブルできることを示している。これらが符号化されたものがIPMP符号化データ1011である。

ビデオ符号化データ1012はIPMP符号化データがセキュリティを施すフレームに対してスクランブルを施すことでセキュリティを実現している。

#### 【0011】

このような符号化データを復号する復号装置の例を図10に示す。

#### 【0012】

図10において、1000は動画像データの符号化データのうち、IPMP符号化データ1011とビデオ符号化データ1012を入力する入力端子である。1001は入力された符号化データをIPMP符号化データ1011とビデオ符号化データ1012に分離する分離器である。1002はバッファであり、分離器1001で分離されたビデオ符号化データ1012を各フレーム単位で格納する。

#### 【0013】

1003はIPMP符号化データを復号するIPMP復号器である。1004は認証を確認する認証器である。1005と1007はセクタであり、認証器1004の出力にしたがって入出力先を変更する。1006はデスクランブラである。1008はビデオの符号化データを復号し、画像データを再生するビデオ復号器である。1009は再生された画像データを出力する出力端子である。

#### 【0014】

上述のように構成された復号装置の動作を以下に説明する。

#### 【0015】

入力端子1000から最初にIPMP符号化データ1011が入力される。分離器1001はこの符号化データをIPMP復号器1003に入力する。IPMP復号器1003はIPMP符号化データ1011を復号し、認証データ、セキュリティの対象となっているフレーム番号やデスクランブルのためのキーを復号する。

#### 【0016】

認証データは認証器1004に入力され、あらかじめ登録された認証データと比較され、認証が正しくなければ常にセクタ1005とセクタ1007を直

結し、デスクランブラ 1 0 0 6 を介さないように指示する。認証が正しければセレクト 1 0 0 5、1 0 0 7 が IPMP 復号器 1 0 0 3 の指示に従ってデスクランブラ 1 0 0 6 を経由するか、しないかを選択する。

【 0 0 1 7 】

この場合では、IPMP 復号器 1 0 0 3 がセキュリティを施すフレームの符号化データと認識した場合、セレクト 1 0 0 5、1 0 0 7 にデスクランブラ 1 0 0 6 を経由するように指示を行う。それ以外の場合はデスクランブル 1 0 0 6 を経由しないように指示する。

【 0 0 1 8 】

すなわち、セレクト 1 0 0 5、1 0 0 7 は認証器 1 0 0 4 が正しく認証できなかった場合、および正しく認証できた場合で IPMP 復号器 1 0 0 3 がデスクランブラ 1 0 0 6 を経由しない場合はお互いを入出力として選択する。また、正しく認証が行え、IPMP 復号器 1 0 0 3 がセキュリティを施すフレームの符号化データと認識した場合はデスクランブラ 1 0 0 6 を経由するように選択する。

【 0 0 1 9 】

従って、正しく認証が行えた場合、ビデオ復号器 1 0 0 8 はセキュリティの施されていないフレームに加えてセキュリティの施されたフレームもデスクランブル処理をデスクランブラ 1 0 0 6 で行っているため、正しい画像を再生することができる。正しく認証できない場合はスクランブルが施された符号化データがビデオ復号器 1 0 0 8 に入力され、ビデオ復号器 1 0 0 8 は正しく復号できないため再生画像は生成されない。

【 0 0 2 0 】

【発明が解決しようとする課題】

しかしながら、このような構成では、ビデオデータを編集する際に必ず IPMP 符号化データを編集する必要が生じ、処理が煩雑になる。たとえば別なシーケンスと組み合わせて 1 つのビットストリームを生成しようとするするとフレーム番号が変わり、IPMP 符号化データも変更する必要が出る。また、スクランブルのためのキー情報をセキュリティの対象となるデータと別に用意する必要があり、冗長な情報を付加することになる。

## 【 0 0 2 1 】

従って、本発明は前記課題を考慮して画像の著作権保護のために画像データを好適に処理する画像データ処理装置及び方法、画像データ処理プログラムが記録されたコンピュータ可読記録媒体を提供することを目的としている。

## 【 0 0 2 2 】

## 【課題を解決するための手段】

上記目的を達成するための本発明による画像処理装置は、画像データを入力する入力手段と、前記画像データを保護するためのセキュリティデータを生成する生成手段と、前記画像データを符号化し、符号化データを生成する符号化手段と、前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される所定符号を抽出する抽出手段と、前記所定符号に前記セキュリティデータを重畳する重畳手段と、前記セキュリティが設定された区間において前記所定符号を除いた前記符号化データにスクランブルを施すスクランブル手段と、前記重畳手段によって処理された所定符号と前記スクランブル手段によって処理された符号化データとを出力する出力手段とを有することを特徴とする。

## 【 0 0 2 3 】

また、上記目的を達成するために本発明の他の態様による画像処理装置は、画像符号化データから一意に決定される所定符号にセキュリティデータが適応的に重畳され、前記所定符号を除いた画像符号化データに前記セキュリティデータに応じて適応的にスクランブル処理されている符号化データを入力する入力手段と、前記符号化データから前記所定符号が存在する位置にある符号を抽出する符号抽出手段と、前記抽出された符号からセキュリティデータを検出する検出手段と、前記検出手段の検出結果に応じて前記符号化データをデスクランブル処理するデスクランブル手段と、前記デスクランブル手段によってデスクランブル処理された画像符号化データを復号化する復号化手段とを有することを特徴とする。

## 【 0 0 2 4 】

また、上記目的を達成するために本発明の他の態様による画像処理方法は、画像データを入力する入力工程と、前記画像データを保護するためのセキュリティ

データを生成する生成工程と、前記画像データを符号化し、符号化データを生成する符号化工程と、前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される所定符号を抽出する抽出工程と、前記所定符号に前記セキュリティデータを重畳する重畳工程と、前記セキュリティが設定された区間において前記所定符号を除いた前記符号化データにスクランブルを施すスクランブル工程と、前記重畳処理された所定符号と前記スクランブル処理された符号化データとを出力する出力工程とを有することを特徴とする。

## 【 0 0 2 5 】

また、上記目的を達成するために本発明の他の態様による画像処理方法は、画像符号化データから一意に決定される所定符号にセキュリティデータが適応的に重畳され、前記所定符号を除いた画像符号化データに前記セキュリティデータに応じて適応的にスクランブル処理されている符号化データを入力する入力工程と、前記符号化データから前記所定符号が存在する位置にある符号を抽出する符号抽出工程と、前記抽出された符号からセキュリティデータを検出する検出工程と、前記検出工程の検出結果に応じて前記符号化データをデスクランブル処理するデスクランブル工程と、前記デスクランブル処理された画像符号化データを復号化する復号化工程とを有することを特徴とする。

## 【 0 0 2 6 】

また、上記目的を達成するために本発明の他の態様による画像処理方法は、階層構造を形成する画像符号化データを入力する入力工程と、前記画像符号化データから所定層の先頭を示す所定コードを抽出する抽出工程と、前記抽出工程によって抽出された所定コードに画像保護のためのセキュリティデータを重畳する重畳工程とを有することを特徴とする。

## 【 0 0 2 7 】

また、上記目的を達成するために本発明の他の態様による画像処理方法は、階層構造を形成する画像符号化データに対して、所定階層の先頭を示す所定コードにセキュリティデータを重畳した符号化データを入力する入力工程と、前記符号化データから前記所定コードが存在する位置にある符号を抽出する抽出工程と、前記抽出された符号から前記セキュリティデータを検出する検出工程と、前記検



出工程の検出結果に応じて前記符号化データを復号化する復号化工程とを有することを特徴とする。

【 0 0 2 8 】

【発明の実施の形態】

以下、本発明の実施例を、図面を用いて詳細に説明する。

【 0 0 2 9 】

<第 1 実施例>

図 1 は、本発明の第 1 の実施例としての画像データ処理装置の構成を示すブロック図である。尚、本実施例では、ビデオの符号化方式として MPEG-4 を用いた場合について説明する。ただし、これに限定されるものではなく、H.261、H.263、MPEG-1、MPEG-2 等およびその他の符号化方式であってももちろんかまわない。

【 0 0 3 0 】

図 1 において、100 は画像データを入力する入力端子であり、1 フレームずつ画像データを入力する。101 は MPEG-4 符号化方式で動画像を符号化するビデオ符号化器である。104 は動画像を保護するセキュリティの設定を行うセキュリティ設定器である。102、112 はセレクタであり、セキュリティ設定器 104 の指示で入出力先を選択する。

【 0 0 3 1 】

103 はバッファであり、符号化データを一時格納する。105 は符号化データの中からスタートコードを検出する検出器である。108 はセキュリティの保護を行うために符号化データに対してスクランブルを行うキーを生成するキー生成器である。110 はセキュリティの解除に必要な認証のデータを設定する認証設定器である。

【 0 0 3 2 】

109 は暗号化器であり、入力されたデータを所定の暗号方式で暗号化して出力する。106 はスタートコードに暗号化されたデータを重畳する暗号重畳器である。107 はスクランブラであり、前述のキーにしたがってスクランブルを行う。111 は合成器であり、暗号重畳器 106 の出力とスクランブラ 107 の出力を合成する。113 は外部からオーディオ符号化データを入力する入力端子で

ある。

【 0 0 3 3 】

1 1 4 はビデオのフレーム単位で音声を多重化する多重化器である。1 1 5 は生成された符号化データを出力する出力端子である。

【 0 0 3 4 】

上述のように構成された画像データ処理装置の動作を以下で説明する。

【 0 0 3 5 】

まず、操作者は、セキュリティ設定器 1 0 4 で著作権を保護するデータの区間を決定し、設定する。ここで説明を容易にするため、フレーム番号 1 から始まる画像データのシーケンスにおいて、フレーム番号  $n$  からフレーム番号  $(n + m)$  に対してセキュリティを施すこととする。

【 0 0 3 6 】

入力端子 1 0 0 からフレーム単位で画像データが入力され、ビデオ符号化器 1 0 1 で符号化され、フレーム単位でセクタ 1 0 2 に入力される。セキュリティ設定器 1 0 4 でセキュリティを施さないフレーム（フレーム番号 1 から  $(n - 1)$ 、またはフレーム番号  $(n + m + 1)$  以上）としていた場合、セクタ 1 0 2 の出力およびセクタ 1 1 2 の入力をバッファ 1 0 3 とする。この場合、符号化データにはスクランブル等のセキュリティは施されず、出力端子 1 1 5 から出力される。

【 0 0 3 7 】

一方、セキュリティ設定器 1 0 4 でセキュリティを施すフレーム（フレーム番号  $n$  から  $(n + m)$ ）としていた場合について述べる。セキュリティ設定器 1 0 4 はキー生成器 1 0 8 に該当するフレームのスクランブルのときに使用するキーを生成させる。生成されたキーはスクランブラ 1 0 7 と暗号化器 1 0 9 に入力される。

【 0 0 3 8 】

また、認証設定器 1 1 0 は認証に必要なデータたとえばパスワードを設定し、暗号化器 1 0 9 に入力する。暗号化器 1 0 9 はこれらを所定の暗号化方式で暗号化し、3 2 ビット以下の暗号データを生成する。本実施例では 2 3 ビットの暗号

データ  $\alpha$  を生成するものとする。

【 0 0 3 9 】

また、セクタ 1 0 2 は出力先をスタートコード検出器 1 0 5 とし、セクタ 1 1 2 は入力先を合成器 1 1 1 とする。従って、セクタ 1 0 2 に入力された符号化データはスタートコード検出器 1 0 5 に入力される。

【 0 0 4 0 】

MPEG-4 で使用されるスタートコードは表 1 に示すとおりである。

【 0 0 4 1 】

【表 1】

符号名	符号 (16 進)
video_object_start_code	00000100~0000011F
video_object_layer_start_code	00000120~0000012F
Reserved	00000130~000001AF
visual_object_sequence_start_code	000001B0
visual_object_sequence_end_code	000001B1
user_data_start_code	000001B2
group_of_vop_start_code	000001B3
video_session_error_code	000001B4
visual_object_start_code	000001B5
vop_start_code	000001B6
Reserved	000001B7~000001B9
face_object_start_code	000001BA
face_object_plane_start_code	000001BB
mesh_object_start_code	000001BC
mesh_object_plane_start_code	000001BD
still_texture_object_start_code	000001BE
texture_spatial_layer_start_code	000001BF
texture_snr_layer_start_code	000001C0
Reserved	000001C1 - C5
System start codes (see note)	000001C6~000001FF

## 【0042】

本実施例では、スタートコード検出器 105 は VOP スタートコード (vop\_start\_code) を検出する。それ以外の符号化データはスクランブラ 107 に入力される。

## 【0043】

検出された VOP スタートコードは暗号重畳器 106 に入力される。暗号重畳器 106 では暗号データ  $\alpha$  を 9 ビット左にシフトし、VOP スタートコードと論理的

排他和をとる。例えば、暗号データ $\alpha$ が16進で“7234A”であったとき暗号重畳器106の出力は“E4715B6”となる。

## 【0044】

キー生成器108で生成されたキーはスクランブラ107に入力され、このキーを使ってスタートコードを除く符号化データに対してスクランブルを施し、合成器111に入力される。合成器111はVOPスタートコードに暗号データ $\alpha$ を重畳した結果を先頭に、スクランブルが施された符号化データと合成する。

## 【0045】

入力端子113からは外部で符号化されたオーディオ符号化データが入力され、フレーム単位でセクタ112から出力されるビデオ符号化データと多重化してパケット化して出力端子115から出力される。

## 【0046】

このような一連の符号化、暗号化、選択処理によりセキュリティを施した符号化データを、冗長を生じることなく実施できる。

## 【0047】

なお、本実施例においては検出する一意の符号としてスタートコードを選択したが、これに限定されず、先頭から固定長または可変長でも一意に符号が検出できる符号であればいかなる符号を検出してもかまわない。

## 【0048】

また、本実施例では検出するスタートコードとしてVOPスタートコードを検出したがこれに限定されず、上位のスタートコードを検出してももちろんかまわない。たとえばレイヤー単位でセキュリティを制御する場合はVOLスタートコード、シーケンス単位で制御する場合はVOSスタートコードに対してキーや認証情報の重畳を行えばよい。

## 【0049】

## &lt;第2実施例&gt;

図2は、本発明の第2の実施例としての画像データ処理装置の構成を示すブロック図である。

## 【0050】

200は符号化データを入力する入力端子である。本実施例では第1実施例で生成された符号化データを処理するものとし、図1の出力端子115に接続されているのと等価である。

【0051】

201は多重化を解く分解器であり、オーディオ符号化データとビデオ符号化データを分離する。ビデオ符号化データはパケット化された単位ごとに後段に出力される。

【0052】

202は出力端子であり、外部のオーディオ復号器にオーディオ符号化データを出力する。203は入力されたビデオ符号化データからVOPスタートコードの位置にある符号化データβを抽出するスタートコード検出器である。204はスタートコードの位置に該当する符号化データ以外の符号化データを格納しておくバッファである。205は符号化データβから正しいVOPスタートコードではない場合、VOPスタートコードとの差異を抽出するエラー解析器である。206は暗号を所定の方式で解読する暗号解読器である。207は認証器であり、符号化データから抽出された認証データと入力された認証データを比較し、同じであった場合にセキュリティの解除を決定する。208は本画像データ処理装置に固有な認証データを格納した認証メモリである。

【0053】

209、211はセレクタであり、認証器207とエラー解析器205の指示に従ってそれぞれの入出力を選択する。210はスクランブルを解除するデスクランブラである。212はビデオ符号化データを復号するビデオ復号器である。213は復号されて再生された画像データを出力する出力端子である。

【0054】

上述のように構成された画像データ処理装置の動作を以下に説明する。

【0055】

入力端子200から入力された符号化データは分離器201に入力される。分離器201はパケット単位の符号化データをビデオ符号化データとオーディオ符号化データとに分離し、オーディオ符号化データを出力端子202から外部に出

力する。

【 0 0 5 6 】

ビデオ符号化データはスタートコード検出器 2 0 3 に入力される。スタートコードである VOP スタートコードは、フレーム単位で符号化されパケット化されたとき必ず先頭の 3 2 ビットに位置している。そのため、先頭から 3 2 ビットの符号化データを抽出してエラー解析器 2 0 5 に出力し、残りをバッファ 2 0 4 に出力する。

【 0 0 5 7 】

エラー解析器 2 0 5 は入力された 3 2 ビットの符号化データと VOP スタートコードを比較し、その差異を求める。すなわち、入力データと VOP スタートコードの値 (000001B6) と論理的排他和を求め、右に 9 ビットシフトする。その結果は暗号解読器 2 0 6 に入力される。

【 0 0 5 8 】

また、VOP スタートコードとまったく同じ、すなわちセキュリティが施されていない場合はセクタ 2 0 9、2 1 1 にそれぞれを直結して入力された符号化データがそのままビデオ復号器 2 1 2 に入力されるように指示する。

【 0 0 5 9 】

また、セキュリティが施されている場合でセクタ 2 0 9、2 1 1 に認証器 2 0 7 の出力が正しく認証されたことを示している場合はデスクランブラ 2 1 0 を経由するように入出力先を制御し、正しく認証できなかった場合にはセクタ 2 0 9、2 1 1 にそれぞれを直結して入力された符号化データがそのままビデオ復号器 2 1 2 に入力されるように指示する。

【 0 0 6 0 】

暗号解読器 2 0 6 は所定の方式で暗号を解読し、スクランブルのキーと認証データを獲得する。この解読方式は第 1 実施例の暗号化器 1 0 9 の暗号を解読する方式を示す。暗号解読によって得られたキーはデスクランブラ 2 1 0 に入力され、認証データは認証器 2 0 7 に入力される。

【 0 0 6 1 】

認証メモリ 2 0 8 は本装置に固有な認証データが格納されている。認証器 2 0

7は暗号解読器206から入力された認証データと認証メモリ208の認証データを比較し、正しく認証できた場合でエラー解析器205で暗号化データの存在が検知できたときにはセクタ209、211はデスクランブラ210での処理を選択させ、そうでなければ直結を指示する。

【0062】

セクタ211からの出力はビデオ復号器212に入力される。ビデオ復号器212は入力データを復号し、再生画像を生成する。この結果、ビデオ復号器212はセキュリティが施されていないフレームに関してはバッファ204、セクタ209、211を介して分離器201からの出力をそのまま入力して復号することで通常の再生画像を得ることができる。

【0063】

また、セキュリティがかかっていた場合、正しく認証ができなければスクランブルされたビデオ符号化データが入力され、スタートコードに暗号データが重畳されているままなのでスタートコードを検出できず、復号ができないため再生画像を得ることはできない。セキュリティがかかっているにもかかわらず正しく認証できればスクランブルが解除され正しい再生画像を得ることが可能になる。

【0064】

このような一連の選択、暗号解読、復号化処理によりセキュリティに対応した画像の再生を実施できる。

【0065】

尚、本実施例ではエラー解析器205の出力を暗号解読器206に入力したが、これに加えてエラーの有無を検証し、エラーがあればビデオ復号器212の動作を停止させるように制御することも可能である。これにより、先頭にスタートコードを検出する機能がなく、誤ったデータでビデオ復号器212が誤動作することを防ぐことができる。

【0066】

<第3実施例>

図3は、本発明の第3の実施例としての画像データ処理装置の構成を示すブロック図である。尚、上述の第1実施例（図1）と同様の構成要素については同一



番号を付してその詳細な説明は省略する。

【 0 0 6 7 】

3 0 1 は操作者が認証データを設定する認証設定器である。3 0 2 はIPMP符号化データを生成するIPMP符号化器である。3 0 3 は暗号化器であり、第1実施例の暗号化器 1 0 9 と同様に暗号化を行うが、キーのみを暗号化する。3 0 4 は第1実施例の暗号重畳器 1 0 6 と同様に暗号化データをスタートコードに重畳する。3 0 5 は多重化器であり、第1実施例の多重化器 1 1 4 の画像データ符号化データとオーディオ符号化データの入力に加え、IPMP符号化データも多重化する。

【 0 0 6 8 】

上述のように構成された画像データ処理の動作を以下で説明する。

【 0 0 6 9 】

まず、操作者は、第1実施例と同様にセキュリティ設定器 1 0 4 で著作権を保護するデータの区間を決定し、設定する。認証設定器 3 0 1 は認証に必要なデータたとえばパスワードを操作者が設定し、IPMP符号化器 3 0 2 に入力する。IPMP符号化器 3 0 2 はIPMPの書式にしたがってビデオ符号化データに対してセキュリティを施すことと認証設定器 3 0 1 で設定された認証に必要なデータを暗号化、符号化する。IPMP符号化器 3 0 2 の出力はビデオ符号化データ、オーディオ符号化データに先駆けて多重化器 3 0 5 で多重化されて出力端子 1 1 5 から出力される。

【 0 0 7 0 】

入力端子 1 0 0 からフレーム単位で画像データが入力され、ビデオ符号化器 1 0 1 で符号化され、フレーム単位でセレクタ 1 0 2 に入力される。セキュリティ設定器 1 0 4 でセキュリティを施さないフレームとしていた場合、第1実施例と同様に符号化データにはスクランブル等のセキュリティは施されず、出力端子 1 1 5 から出力される。

【 0 0 7 1 】

次に、セキュリティ設定器 1 0 4 でセキュリティを施すフレームとしていた場合について述べる。

【 0 0 7 2 】

セキュリティ設定器 1 0 4 はキー生成器 1 0 8 に該当するフレームのスクランブルのときに使用するキーを生成させる。生成されたキーはスクランブラ 1 0 7 と暗号化器 3 0 3 に入力される。また、暗号化器 3 0 3 は前記キーを所定の暗号化方式で暗号化し、3 2 ビット以下の暗号データを生成する。本実施例では 3 2 ビットの暗号データ  $\gamma$  を生成するものとする。

## 【 0 0 7 3 】

セレクタ 1 0 2 は出力先をスタートコード検出器 1 0 5 とし、セレクタ 1 1 2 は入力先を合成器 1 1 1 とする。従って、セレクタ 1 0 2 に入力された符号化データはスタートコード検出器 1 0 5 に入力される。スタートコード検出器 1 0 5 は VOP スタートコードを検出する。それ以外の符号化データはスクランブラ 1 0 7 に入力される。検出された VOP スタートコードは暗号重畳器 3 0 4 に入力される。暗号重畳器 3 0 4 では暗号データ  $\gamma$  を VOP スタートコードと論理的排他和をとる。例えば暗号データ  $\gamma$  が 1 6 進で “7234A19C” であったとき暗号重畳器 3 0 4 の出力は “7234A02A” となる。

## 【 0 0 7 4 】

キー生成器 1 0 8 で生成されたキーはスクランブラ 1 0 7 に入力され、このキーを使ってスタートコードを除く符号化データに対してスクランブルを施し、合成器 1 1 1 に入力される。合成器 1 1 1 は VOP スタートコードに暗号データ  $\gamma$  を重畳した結果を先頭に、スクランブルが施された符号化データと合成する。

## 【 0 0 7 5 】

出力端子 1 1 5 からは外部で符号化されたオーディオ符号化データが入力され、多重化器 3 0 5 でフレーム単位でセレクタから出力されるビデオ符号化データと多重化してパケット化して出力端子 1 1 5 から出力される。

## 【 0 0 7 6 】

上述のような一連の符号化、暗号化、選択処理によりセキュリティを施した符号化データを、冗長を生じることなく実施できる。ビデオのセキュリティの詳細はビデオの符号化データ内に内包し、全体を IPMP で管理することにより、ビデオデータの管理を容易にすることもできる。

## 【 0 0 7 7 】

#### ＜第 4 実施例＞

図 4 は、本発明の第 4 の実施例としての画像データ処理装置の構成を示すブロック図である。尚、上述の第 2 実施例（図 2）と同様の構成要素については同一番号を付してその詳細な説明は省略する。また、本実施例では第 3 実施例で生成された符号化データを処理するものとし、図 4 の入力端子 2 0 0 は図 3 の出力端子 1 1 5 に接続されているのと等価である。

#### 【 0 0 7 8 】

図 4 において、4 0 1 は多重化を解く分離器であり、IPMP符号化データ、オーディオ符号化データ、ビデオ符号化データを分離する。ビデオ符号化データはパケット化された単位ごとに後段に出力される。4 0 2 は IPMP 復号器であり、IPMP 情報を復号する。

#### 【 0 0 7 9 】

4 0 3 は操作者が認証データを入力するための端末である。4 0 4 はスタートコード検出器 2 0 3 で抽出された符号化データと VOP スタートコードとの差異を抽出するエラー解析器である。4 0 5 は暗号を所定の方式で解読する暗号解読器である。4 0 6 はビデオ復号器であり、再生画像のデータと正しく復号できたか否かを出力する。4 0 7 はフレームメモリであり、最後に正しく復号された画像データを 1 フレーム分保持する。4 0 8 はセレクタであり、ビデオ復号器 4 0 6 の復号結果にしたがってビデオ復号器 4 0 6 からの出力かフレームメモリ 4 0 7 からの出力かを選択して出力する。

#### 【 0 0 8 0 】

上述のように構成された画像データ処理装置の動作を以下で説明する。

#### 【 0 0 8 1 】

入力端子 2 0 0 から入力された符号化データは分離器 4 0 1 に入力される。分離器 4 0 1 は IPMP 符号化データとパケット単位の符号化データをビデオ符号化データとオーディオ符号化データとに分離する。そのうち、オーディオ符号化データを出力端子 2 0 2 から外部に出力する。

#### 【 0 0 8 2 】

IPMP 符号化データは IPMP 復号器 4 0 2 に出力される。IPMP 復号器 4 0 2 は IPMP

符号化データを復号し、IPMPに関する情報、この場合はシーケンスに関する認証データを復号して獲得する。認証データは認証器 2 0 7 に入力され端末 4 0 3 からの操作者による認証データの入力を促す。

【 0 0 8 3 】

また、分離器 4 0 1 で分離されたビデオ符号化データはスタートコード検出器 2 0 3 に入力され、第 2 実施例と同様にスタートコードに該当する符号化データとそれ以外を分離し、スタートコードに該当するデータをエラー解析器 4 0 4 に、それ以外をバッファ 2 0 4 に出力する。

【 0 0 8 4 】

認証器 2 0 7 は端末 4 0 3 から入力された認証データと IPMP 復号器 4 0 2 から入力された認証データを比較し、正しく認証できた場合でエラー解析器 4 0 4 で暗号化データの存在が検知できたときにはセレクタ 2 0 9、2 1 1 はデスクランブラ 2 1 0 での処理を選択させ、そうでなければ直結を指示する。

【 0 0 8 5 】

エラー解析器 4 0 4 は入力された 3 2 ビットの符号化データと VOP スタートコードを比較し、その差異を求める。すなわち、入力データと VOP スタートコードの値 (000001B6) と論理的排他和を求める。その結果は暗号解読器 4 0 5 に入力される。

【 0 0 8 6 】

また、セキュリティが施されていない場合はセレクタ 2 0 9、2 1 1 にそれぞれを直結して入力された符号化データがそのままビデオ復号器 4 0 6 に入力されるように指示する。

【 0 0 8 7 】

また、セキュリティが施されている場合でセレクタ 2 0 9、2 1 1 に認証器 2 0 7 の出力が正しく認証されたことを示している場合はデスクランブラ 2 1 0 を経由するように入出力先を制御し、正しく認証できなかった場合にはセレクタ 2 0 9、2 1 1 にそれぞれを直結して入力された符号化データがそのままビデオ復号器 4 0 6 に入力されるように指示する。

【 0 0 8 8 】

暗号解読器 4 0 5 は所定の方式で暗号を解読し、スクランブルのキーを獲得する。暗号解読によって得られたキーはデスクランブラ 2 1 0 に入力される。

#### 【 0 0 8 9 】

セレクタ 2 1 1 からの出力はビデオ復号器 4 0 6 に入力される。ビデオ復号器 4 0 6 は入力データを復号し、再生画像を生成する。この結果、ビデオ復号器 4 0 6 はセキュリティが施されていないフレームに関してはバッファ 2 0 4、セレクタ 2 0 9、2 1 1 を介して分離器 4 0 1 からの出力をそのまま入力して復号することで通常の再生画像を得ることができる。このデータはセレクタ 4 0 8 を介して出力端子 2 1 3 から外部に出力され、同時にフレームメモリ 4 0 7 に格納される。

#### 【 0 0 9 0 】

また、セキュリティが施されていた場合、正しく認証ができなければスクランブルされたビデオ符号化データが入力され、スタートコードに暗号データが重畳されているままなのでスタートコードを検出できず、復号ができない。この場合、セレクタ 4 0 8 は正しく復号された最後のフレームデータをフレームメモリ 4 0 7 から読み出し、端子 2 1 3 に出力する。この時、フレームメモリ 4 0 7 の内容は更新されない。

#### 【 0 0 9 1 】

セキュリティがかかっているにもかかわらず正しく認証できればスクランブルが解除され正しい再生画像を得ることが可能になる。この場合もセレクタ 4 0 8 を介して出力端子 2 1 3 から外部に出力され、同時にフレームメモリ 4 0 7 に格納される。

#### 【 0 0 9 2 】

このような一連の選択、暗号解読、復号化処理によりセキュリティに対応した画像の再生を実施できる。画像のスクランブルに関する情報をビデオの符号化データに重畳してあるのでフレーム単位での管理も容易になる。さらに、復号ができない場合でも正しく再生された画像を出すことで、いきなり画像が表示されなくなったり、ノイズ画面が出たりしなくなったので、操作者に不快感を与えないようにすることができる。

#### 【 0 0 9 3 】

## ＜第 5 実施例＞

図 5 は、本発明の第 5 の実施例としての画像データ処理装置の構成を示すブロック図である。尚、本実施例では特に画像データの符号化処理について説明する。また、本実施例では MPEG-1 符号化方式を例にとって説明するが、特にこれに限定されることではない。MPEG-1 の詳細な仕様については ISO 11172-2 を参照されたい。

## 【 0 0 9 4 】

図 5 において、5 0 0 は装置全体の制御、及び種々の処理を行う中央演算装置 (CPU)、5 0 1 は本装置の制御に必要なオペレーティングシステム (OS)、ソフトウェア、演算に必要な記憶領域を提供するメモリである。尚、メモリ 5 0 1 には装置全体を制御し、各種ソフトウェアを動作させるための OS や動作させるソフトウェアを格納し、画像データを符号化のために読み込む画像エリア、一時的に符号データを格納する符号エリア、各種演算のパラメータ等を格納しておくワーキングエリアが存在する。

## 【 0 0 9 5 】

5 0 2 は種々の装置をつなぎ、データ、制御信号をやり取りするバス、5 0 3 はソフトウェアを蓄積する記憶装置、5 0 4 は動画像データを蓄積する記憶装置、5 0 5 は画像を表示するモニタであり、5 0 8 は通信回路であり、LAN、公衆回線、無線回線、放送電波等で構成されている。5 0 7 は通信回路 5 0 8 に符号化データを送信する通信インターフェースである。5 0 6 は装置を起動したり、セキュリティを設定したりするための端末である。

## 【 0 0 9 6 】

上述のように構成においてまず、処理に先立ち、端末 5 0 6 から記憶装置 5 0 4 に蓄積されている動画像データから符号化する動画像データを選択し、装置の起動が指示される。すると記憶装置 5 0 3 に格納されているソフトウェアがバス 5 0 2 を介してメモリ 5 0 1 に展開され、ソフトウェアが起動される。

## 【 0 0 9 7 】

以下、CPU 5 0 0 による記憶装置 5 0 4 に格納されている動画像データの符号化動作を図 6、図 7 に示すフローチャートに従って説明する。

## 【 0 0 9 8 】

まず、図 6 を用いて符号化処理を説明する。

## 【 0 0 9 9 】

図 6 において、ステップ S 1 ではシーケンス単位で認証を行う「シーケンス認証データ」、シーンの集合単位で認証を行う「シーン認証データ」、セキュリティを施して復号の禁止を開始するピクチャ、禁止を解除するピクチャ、ピクチャ単位での認証を行う「ピクチャ認証データ」などのセキュリティの設定条件を入力し、これらをメモリ 5 0 1 のワーキングエリアに格納し、ステップ S 2 に進む。

## 【 0 1 0 0 】

ステップ S 2 では「シーケンス認証データ」を暗号化し、MPEG-1 符号化方式のシーケンスヘッダコード（値 “000001B3”）に排他的論理和によって重畳し、メモリ 5 0 1 の所定の領域に格納し、ステップ S 3 に進む。

## 【 0 1 0 1 】

ステップ S 3 では他のシーケンスレイヤの符号化データを生成し、重畳されたシーケンスヘッダコードに続けて格納し、パケットとして記憶装置 5 0 4 の所定の領域に蓄積し、ステップ S 4 に進む。

## 【 0 1 0 2 】

ステップ S 4 では GOP を 1 つのシーンとして考えたとき、符号化対象の全シーンの画像データについて処理を終了したか否かを判定する。もし全ての画像データの処理が終了していればソフトウェアを終了する。そうでなければ、ステップ S 5 に進む。

## 【 0 1 0 3 】

ステップ S 5 では「GOP 認証データ」を暗号化し、MPEG-1 符号化方式の GOP スタートコード（値 “000001B7”）に排他的論理和によって重畳し、メモリ 5 0 1 の所定の領域に格納し、ステップ S 6 に進む。

## 【 0 1 0 4 】

ステップ S 6 では他の GOP レイヤの符号化データを生成し、重畳された GOP スタートコードに続けて格納し、パケットとして記憶装置 5 0 4 の所定の領域に蓄積

し、ステップ S 7 に進む。

【 0 1 0 5 】

ステップ S 7 では GOP 内の符号化対象の全ピクチャ画像データについて符号化処理を終了したか否かを判定する。もし全ての画像データの符号化処理が終了していれば GOP の符号化処理を終了し、次の GOP の符号化処理をするため、ステップ S 4 に進む。そうでなければ、ステップ S 8 に進み、各ピクチャ単位の符号化を行う。

【 0 1 0 6 】

次に、図 6 のステップ S 8 の各ピクチャ単位での符号化処理を図 7 を用いて説明する。

【 0 1 0 7 】

図 7 において、ステップ S 1 0 では、図 6 のステップ S 1 で設定してメモリ 5 0 1 上のワーキングエリアに格納されたピクチャの条件にしたがって、符号化対象のピクチャ画像データがセキュリティを施す必要があるか否かを判定する。もし符号化するピクチャがセキュリティを施す区間に含まれていれば暗号化処理を行うため、ステップ S 1 2 に進む。そうでなければ、ステップ S 1 1 に進み、通常どおりのピクチャの符号化を行う。

【 0 1 0 8 】

ステップ S 1 1 では記憶装置 5 0 4 から符号化するピクチャの画像データを読み出し、MPEG-1 符号化方式のピクチャレイヤの符号化を行い、パケットとして記憶装置 5 0 4 の所定の領域に蓄積し、次のピクチャの処理をするため、図 6 のステップ S 7 に進む。

【 0 1 0 9 】

ステップ S 1 2 ではスクランブルのためのキーを生成し、生成したキーと「ピクチャ認証データ」を暗号化し、MPEG-1 符号化方式のピクチャスタートコード（値“00000100”）に排他的論理和によって重畳し、メモリ 5 0 1 の所定の領域に格納し、ステップ S 1 3 に進む。

【 0 1 1 0 】

ステップ S 1 3 では他のピクチャレイヤのヘッダに関する符号化データを生成



し、重畳されたピクチャスタートコードに続けて格納する。さらに記憶装置 5 0 4 から符号化するピクチャの画像データを読み出し、符号化してメモリ 5 0 1 の符号エリアに一時的に格納する。

【 0 1 1 1 】

ステップ S 1 4 ではステップ S 1 3 で生成した符号化データに対して、ステップ S 1 2 で生成したキーを使ってスクランブル処理を行いステップ S 1 5 に進む。

【 0 1 1 2 】

ステップ S 1 5 では重畳されたピクチャスタートコードとスクランブルされた符号化データをパケットとして記憶装置 5 0 4 の所定の領域に蓄積し、ステップ S 7 に進む。

【 0 1 1 3 】

上述のような一連の符号化、暗号化、選択処理によりセキュリティを施した符号化データを、冗長データを発生することなく実施できる。各レイヤでセキュリティを行うことができるのでさまざまなレベルのセキュリティに対応することもできる。

【 0 1 1 4 】

尚、上述の実施例では記憶装置 5 0 4 に蓄積する例を述べたが、通信インターフェース 5 0 5 を介して通信回線 5 0 6 に送出してもよい。

【 0 1 1 5 】

< 第 6 実施例 >

本実施例では特に画像データの復号化処理について説明する。画像データ処理装置の構成は第 5 実施例の図 5 と同様である。尚、本実施例においても MPEG-1 符号化方式を例にとって説明するが、特にこれに限定されることではない。また、本実施例では第 5 実施例で生成され、記憶装置 5 0 4 に格納された符号化データの復号処理を例にとって説明する。

【 0 1 1 6 】

図 5 の構成において、処理に先立ち、端末 5 0 6 から記憶装置 5 0 4 に蓄積されている動画像符号化データから復号する符号化データを選択し、装置の起動が

指示されると記憶装置 5 0 3 に格納されているソフトウェアがバス 5 0 2 を介してメモリ 5 0 1 に展開され、ソフトウェアが起動される。

【 0 1 1 7 】

以下、CPU 5 0 0 による記憶装置 5 0 4 に格納されている符号化データの復号動作を図 8、図 9 に示すフローチャートに従って説明する。

【 0 1 1 8 】

まず、図 8 を用いて復号化処理を説明する。

【 0 1 1 9 】

図 8 において、ステップ S 2 0 では記憶装置 5 0 4 から復号するシーケンスの最初の packets を読み出し、メモリ 5 0 1 の符号エリアに格納する。格納された符号化データから先頭の 3 2 ビットをシーケンスヘッダコードと比較し、重畳された「シーケンス認証データ」を分離し、暗号を解読し、ステップ S 2 1 に進む。

【 0 1 2 0 】

ステップ S 2 1 では解読された「シーケンス認証データ」と端末 5 0 6 から入力された認証データと比較し、正しく認証された場合ステップ S 2 2 に進み、復号処理を継続する。正しく認証されない場合は復号処理を終了し、ソフトウェアを終了する。

【 0 1 2 1 】

ステップ S 2 2 ではメモリ 5 0 1 の符号エリアに格納された他のシーケンスレイアの符号化データを復号し、後段の処理でできるように、その結果をメモリ 5 0 1 のワーキングエリアに格納し、ステップ S 2 3 に進む。

【 0 1 2 2 】

ステップ S 2 3 では全シーン (GOP) の画像データについて処理を終了したか否かを判定する。もし全ての画像データの処理が終了していればソフトウェアを終了する。そうでなければ、ステップ S 2 4 に進む。

【 0 1 2 3 】

ステップ S 2 4 では記憶装置 5 0 4 から復号する GOP のヘッダに関する packets を読み出し、メモリ 5 0 1 の符号エリアに格納する。格納された符号化データ

から先頭の 3 2 ビットを GOP スタートコードと比較し、重畳された「GOP 認証データ」を分離し、暗号を解読し、ステップ S 2 5 に進む。

【 0 1 2 4 】

ステップ S 2 5 では解読された「GOP 認証データ」と端末 5 0 6 から入力された認証データと比較し、正しく認証された場合はステップ S 2 6 に進み、復号処理を継続する。正しく認証されない場合はステップ S 2 3 に進み、次の GOP の処理を試みる。

【 0 1 2 5 】

ステップ S 2 6 ではメモリ 5 0 1 の符号エリアに格納された他の GOP レイヤの符号化データを復号し、後段の処理でできるように、その結果をメモリ 5 0 1 のワーキングエリアに格納し、ステップ S 2 7 に進む。

【 0 1 2 6 】

ステップ S 2 7 では GOP 内の復号対象の全ピクチャ画像データについて処理を終了したか否かを判定する。もし全ての画像データの復号処理が終了していれば GOP の復号処理を終了し、次の GOP の復号処理をするため、ステップ S 2 3 に進む。そうでなければ、ステップ S 2 8 に進み、各ピクチャ単位の復号を行う。

【 0 1 2 7 】

次に、図 8 のステップ S 2 8 の各ピクチャ単位での復号化処理を図 9 を用いて説明する。

【 0 1 2 8 】

図 9 において、ステップ S 3 1 では記憶装置 5 0 4 から復号するピクチャに関するパケットを読み出し、メモリ 5 0 1 の符号エリアに格納する。

【 0 1 2 9 】

ステップ S 3 2 ではメモリ 5 0 1 に格納された符号化データから先頭の 3 2 ビットをピクチャスタートコードと比較し、値が“00000100”であればステップ S 3 3 に進み、通常どおりのピクチャの復号を行う。すなわちセキュリティは施されていない。また値が“00000100”でなければセキュリティが施されているとし、ステップ S 3 4 に進み、処理を行う。

【 0 1 3 0 】

ステップ S 3 3 ではメモリ 5 0 1 の符号エリアから復号するピクチャの符号化データを読み出し、MPEG-1符号化方式のピクチャレイヤの復号を行い、モニタ 5 0 5 に送られ、表示される。さらに次のピクチャの処理をするため、図 8 のステップ S 2 7 に進む。

【 0 1 3 1 】

一方、ステップ S 3 4 では重畳された「ピクチャ認証データ」とスクランブルのキーを分離し、暗号を解読し、ステップ S 3 5 に進む。

【 0 1 3 2 】

ステップ S 3 5 では解読された「ピクチャ認証データ」と端末 5 0 6 から入力された認証データと比較し、正しく認証された場合ステップ S 3 6 に進み、復号処理を継続する。正しく認証されない場合は次のピクチャの処理をするため、図 8 のステップ S 2 7 に進む。

【 0 1 3 3 】

ステップ S 3 6 ではメモリ 5 0 1 の符号エリアに格納されたピクチャレイヤの符号化データを読み出しスクランブルを暗号解読によって得られたキーでデスクランブルし、ステップ S 3 7 に進む。

【 0 1 3 4 】

ステップ S 3 7 ではデスクランブルされたピクチャの符号化データを MPEG-1 符号化方式のピクチャレイヤの復号を行い、モニタ 5 0 5 に送り、表示する。さらに次のピクチャの処理をするため、図 8 のステップ S 2 7 に進む。

【 0 1 3 5 】

このような一連の選択、暗号解読、復号化処理によりセキュリティに対応した画像の再生を実施できる。

【 0 1 3 6 】

各レイヤでセキュリティを行うことができるのでさまざまなレベルのセキュリティに対応でき、それぞれの認証データの解読ができないシステムでは各スタートコードを認識できないため、まったく再生を行うことはできず、著作権を保護することができる。

【 0 1 3 7 】

【発明の効果】

以上の説明から明らかなように、本発明では、冗長データの付加を抑えながらセキュリティを施した符号化データを生成することができる。

【0138】

また、本発明ではセキュリティデータを階層に応じて設定することも可能となる。ピクチャやフレーム単位で管理が行えるので編集等にも好適に扱うことができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施例としての画像データ処理装置の構成を示すブロック図である。

【図2】

本発明の第2の実施例としての画像データ処理装置の構成を示すブロック図である。

【図3】

本発明の第3の実施例としての画像データ処理装置の構成を示すブロック図である。

【図4】

本発明の第4の実施例としての画像データ処理装置の構成を示すブロック図である。

【図5】

本発明の第5及び第6の実施例としての画像データ処理装置の構成を示すブロック図である。

【図6】

本発明の第5実施例における画像の符号化の工程を現すフローチャート図である。

【図7】

本発明の第5実施例における画像の符号化の工程を現すフローチャート図である。

【図 8】

本発明の第 6 実施例における画像の復号の工程を現すフローチャート図である

【図 9】

本発明の第 6 実施例における画像の復号の工程を現すフローチャート図である

【図 1 0】

従来例を示すブロック図である。

【図 1 1】

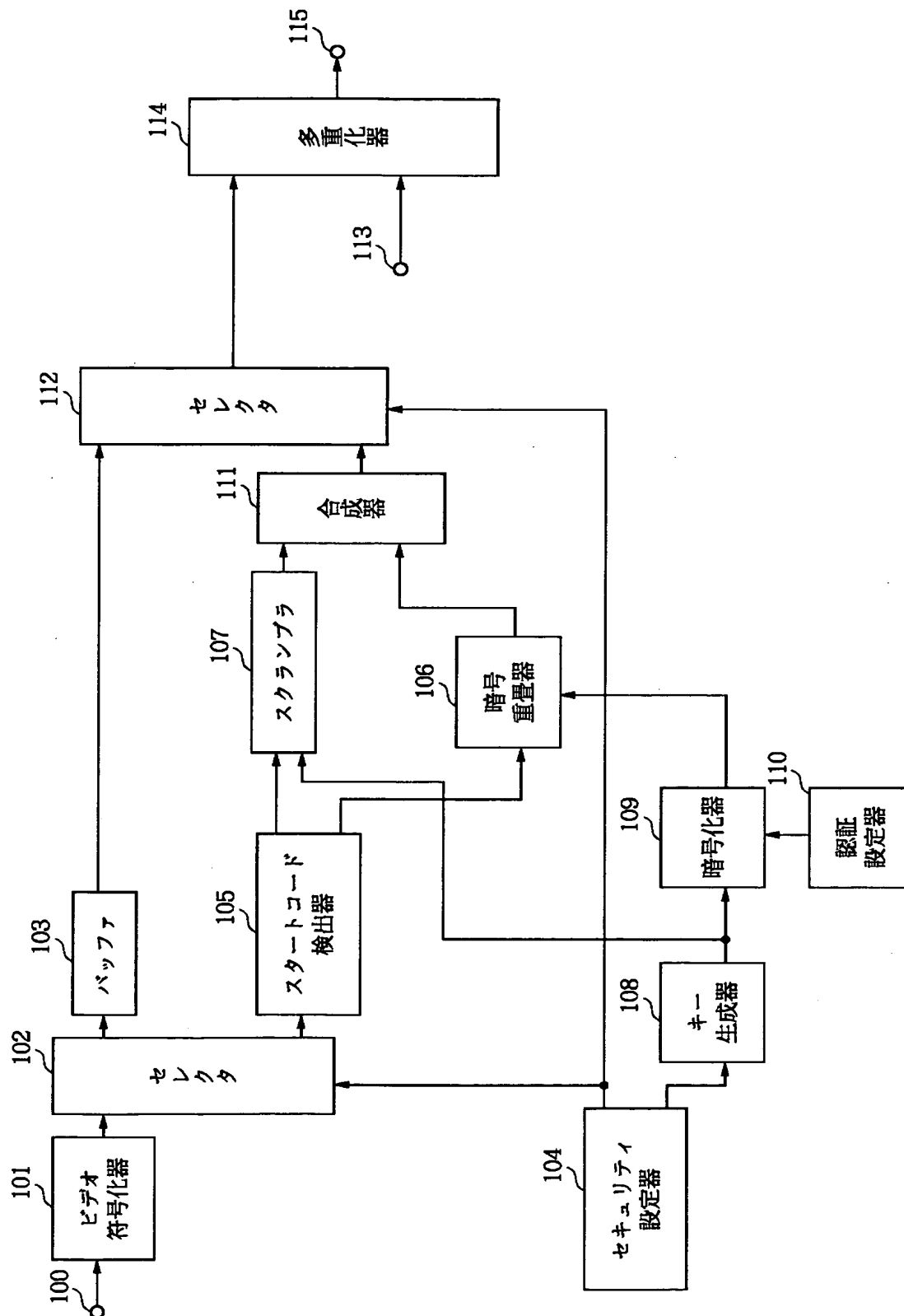
MPEG-4のビットストリームの構成例を示す図である。

【図 1 2】

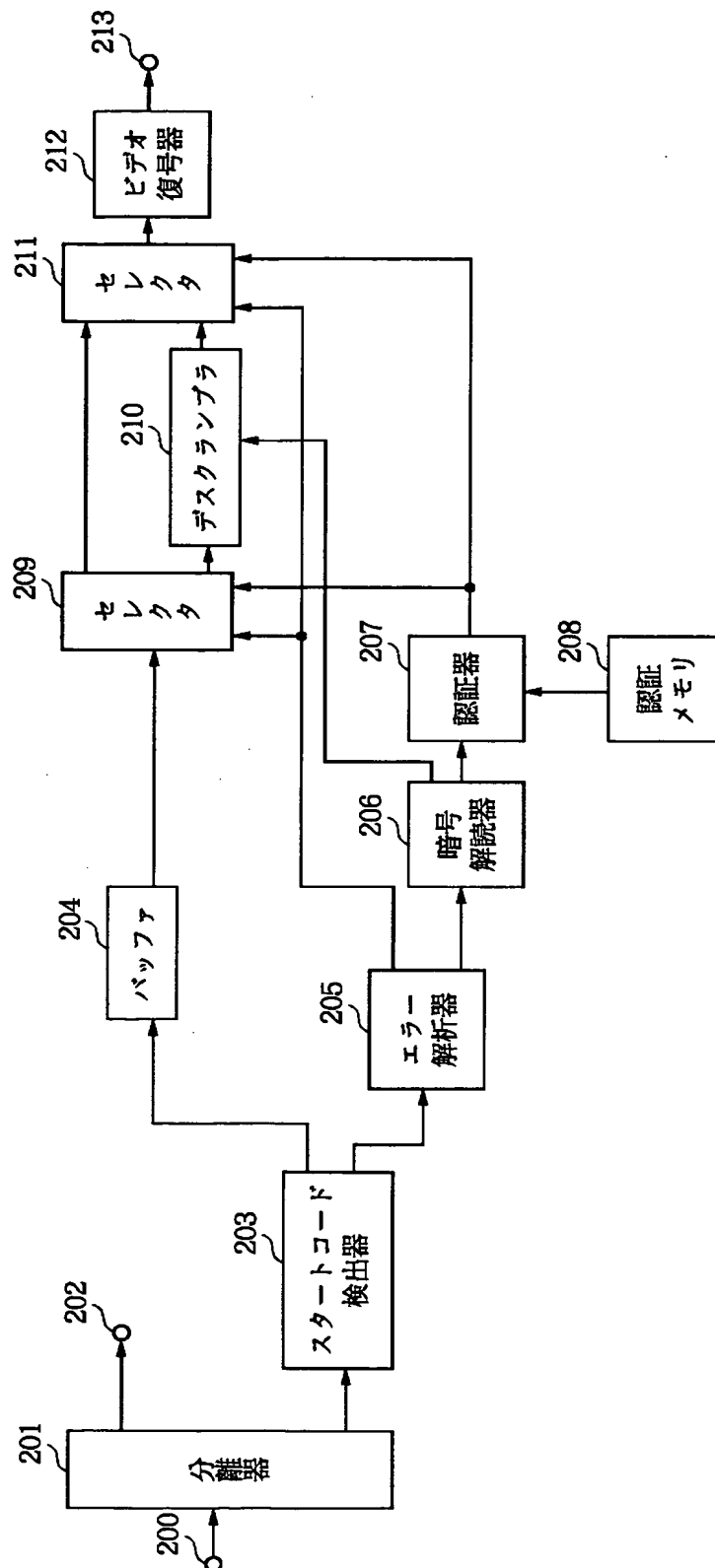
IPMP符号化データに含まれる情報の例を示す図である。

【書類名】 図面

【図 1】

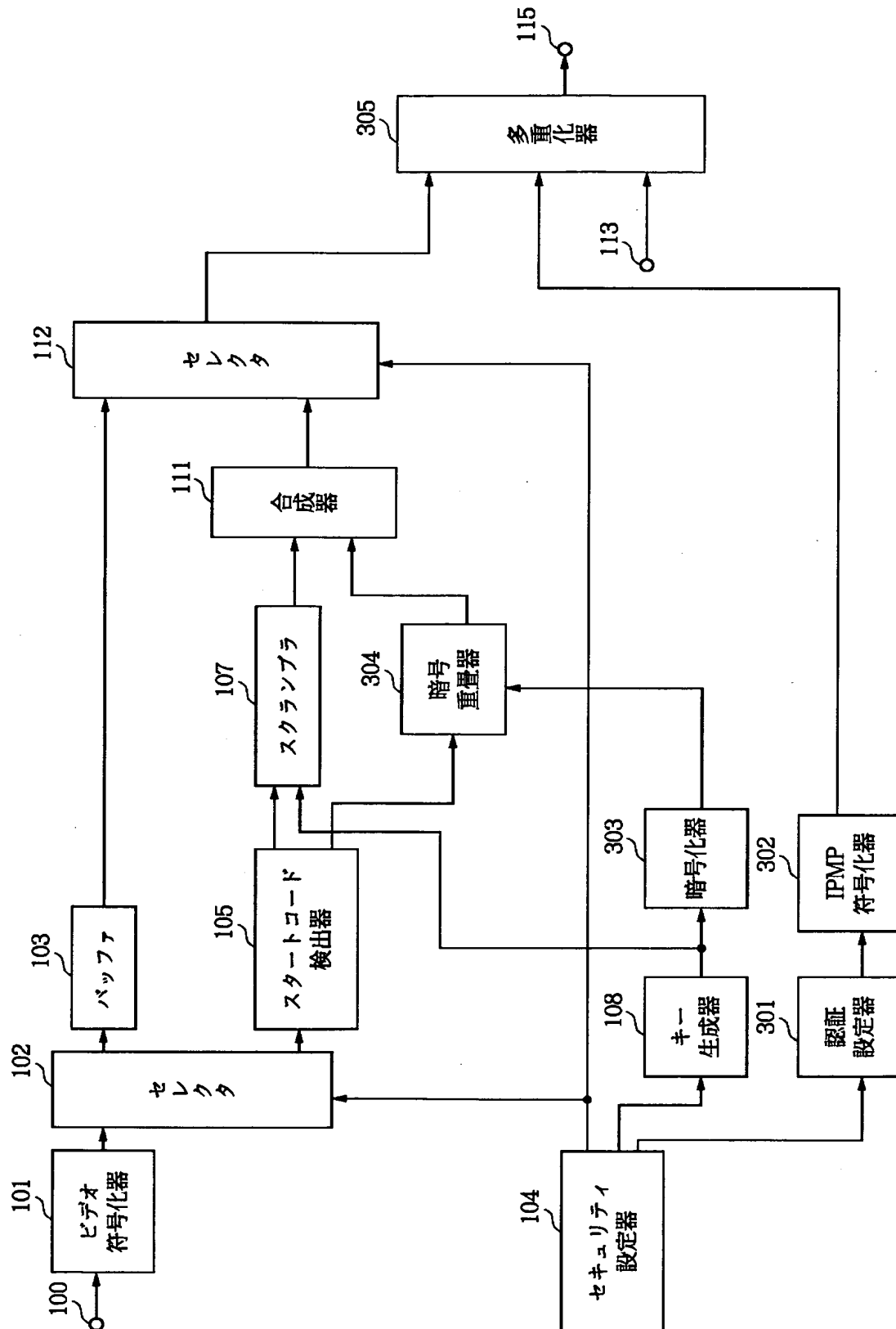


【図 2】

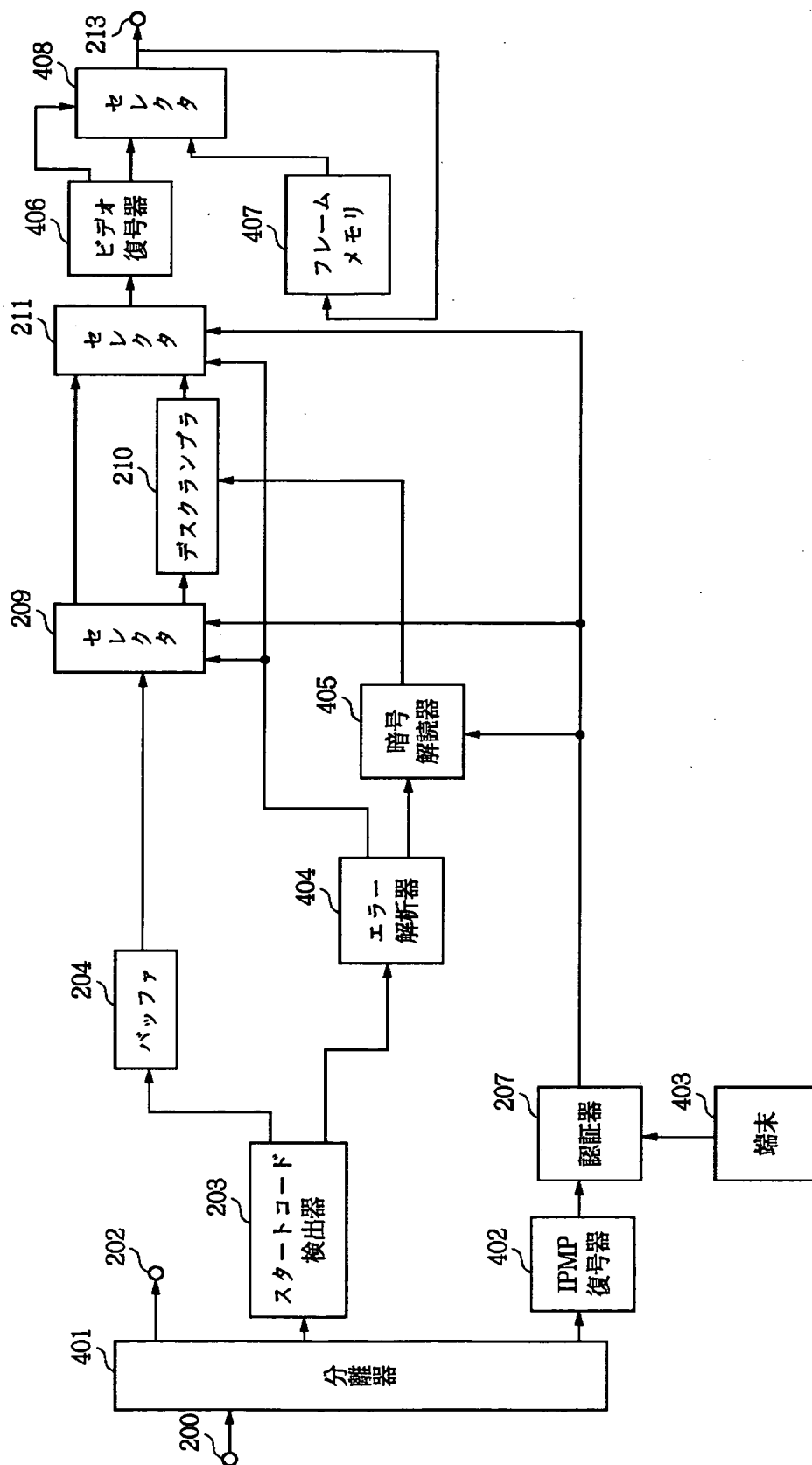




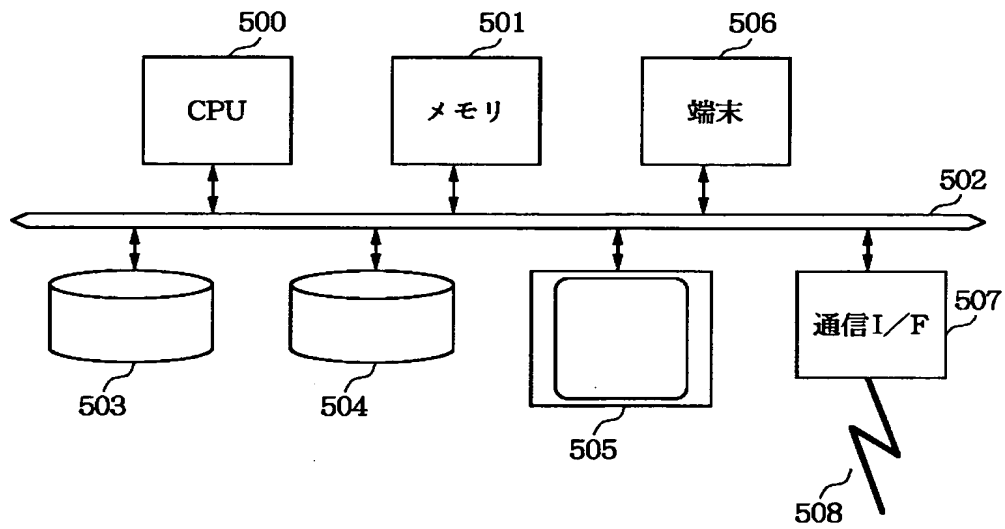
【図 3】



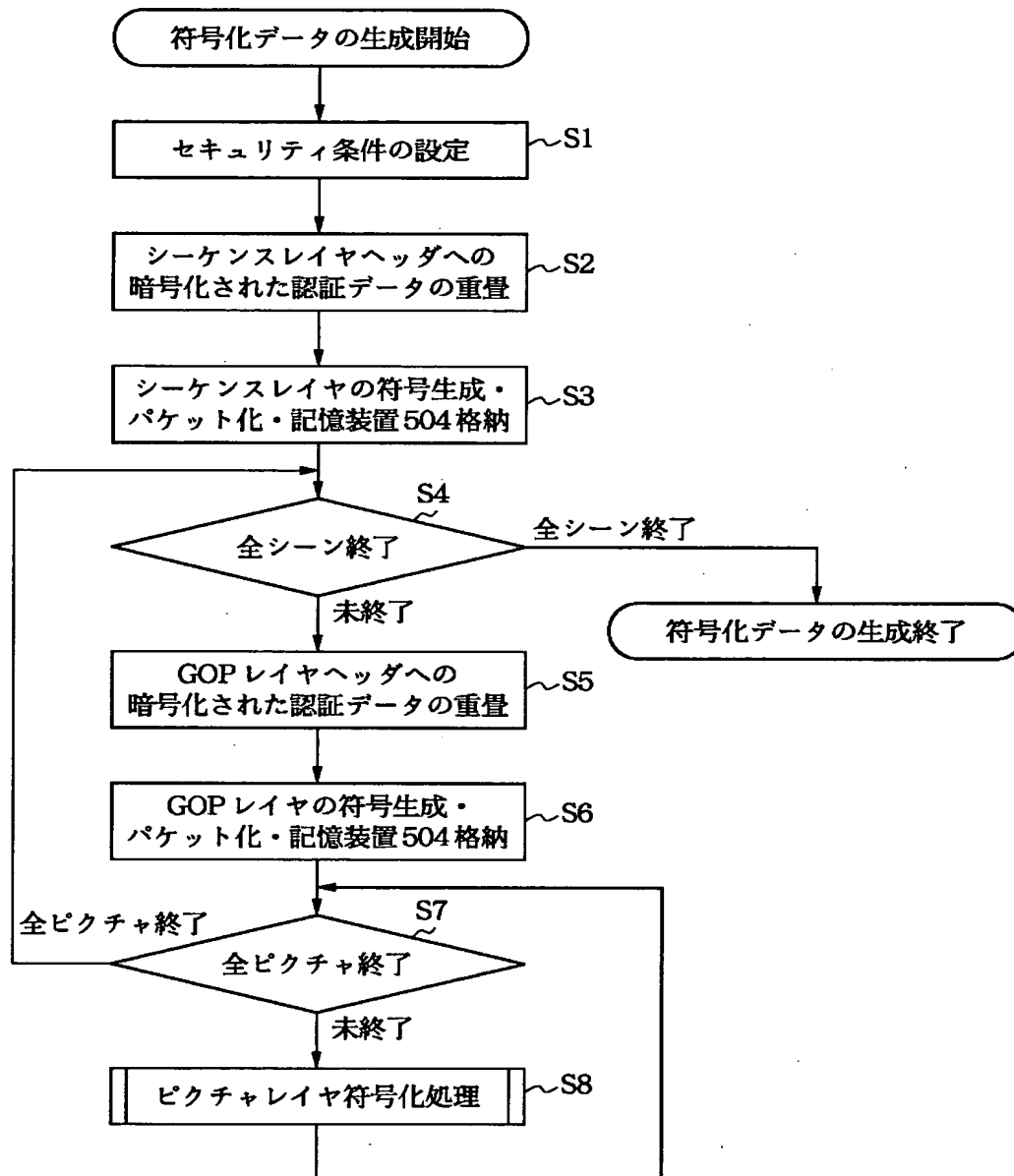
【図 4】



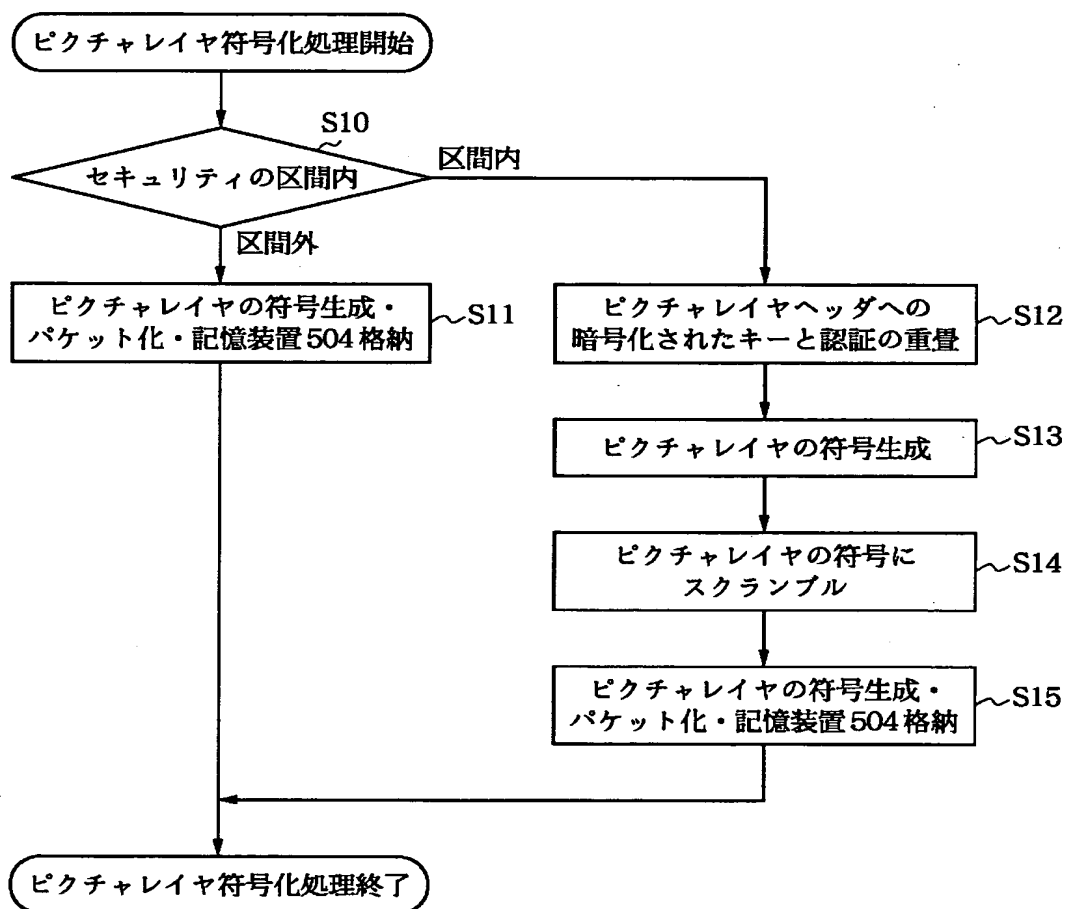
【図 5】



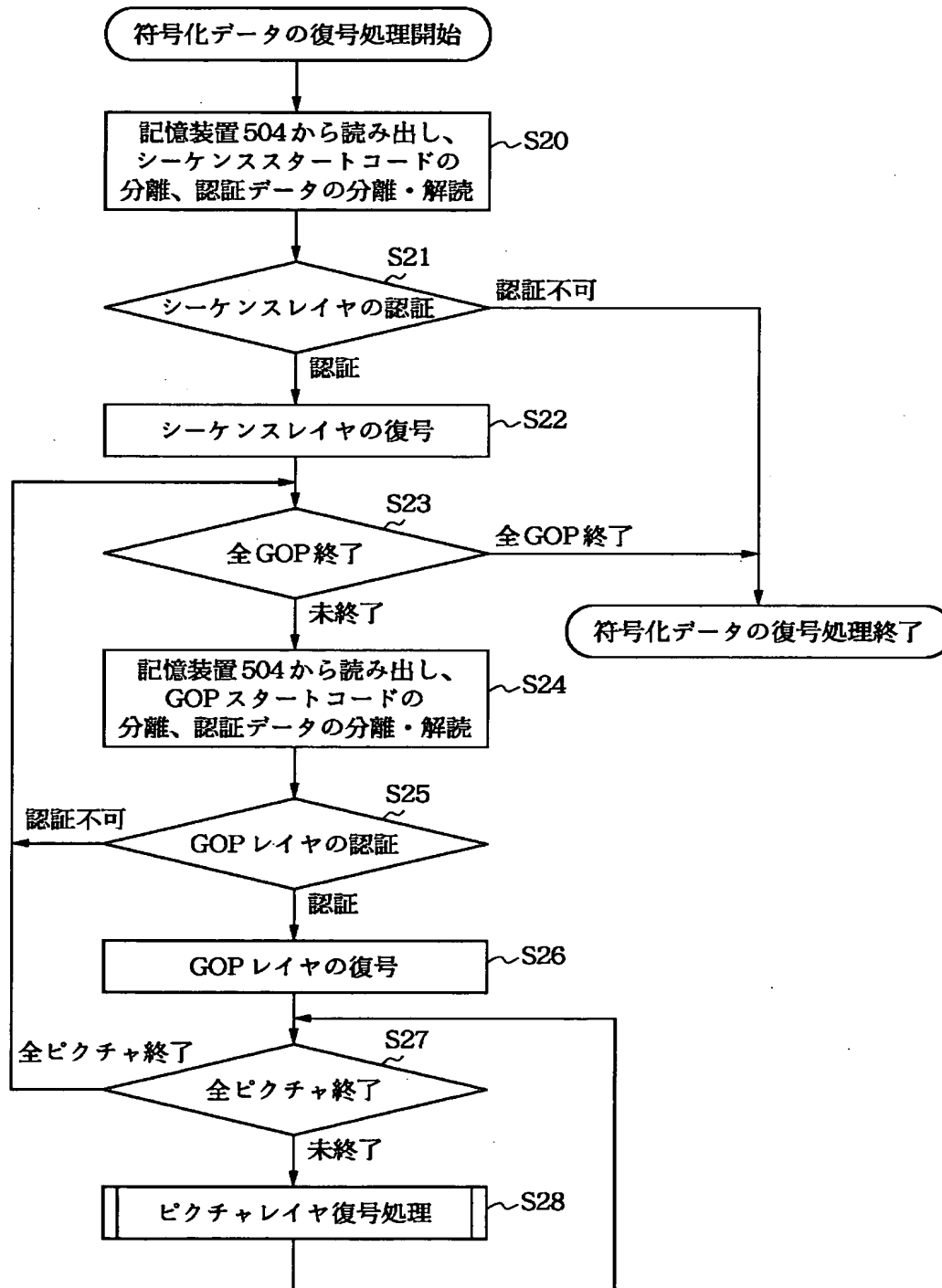
【図 6】



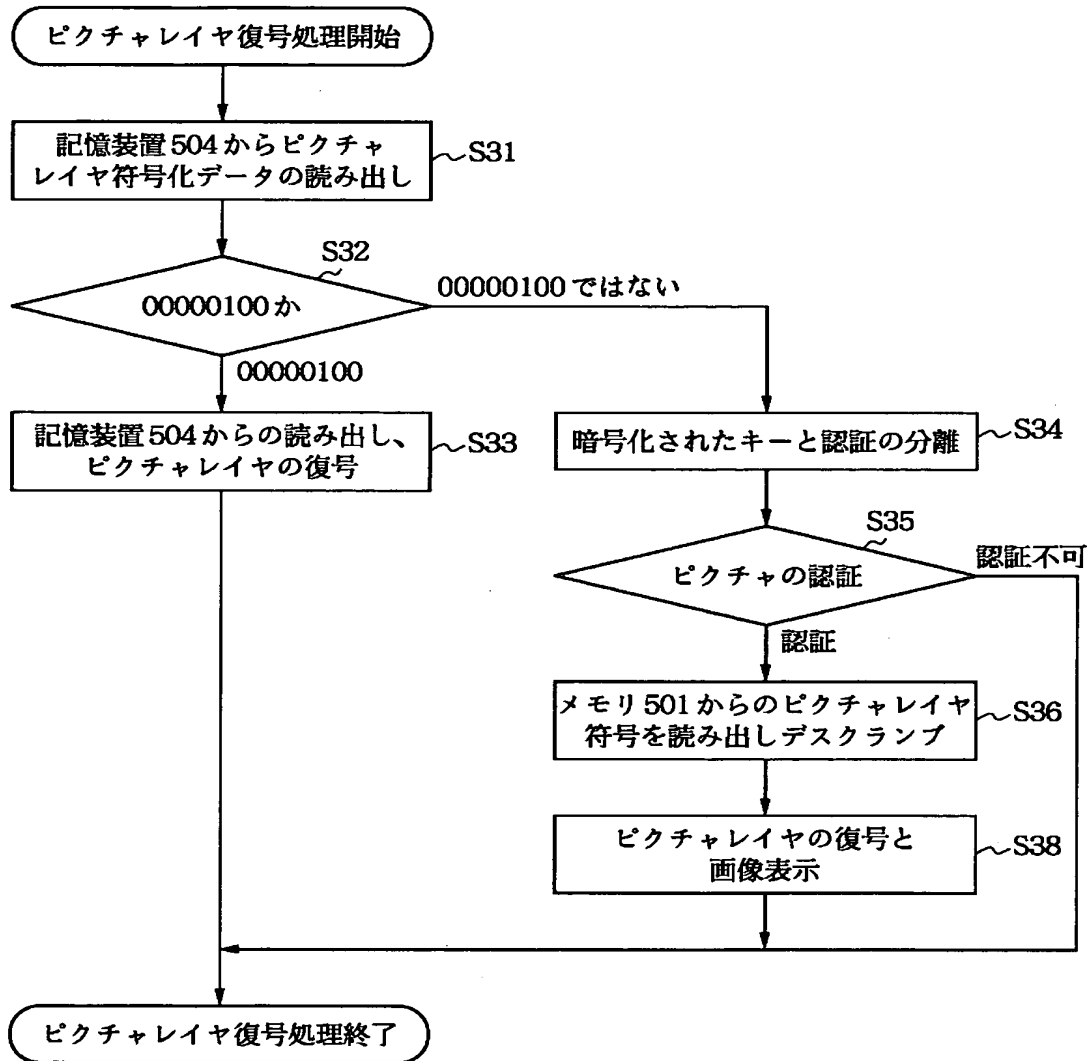
【図 7】



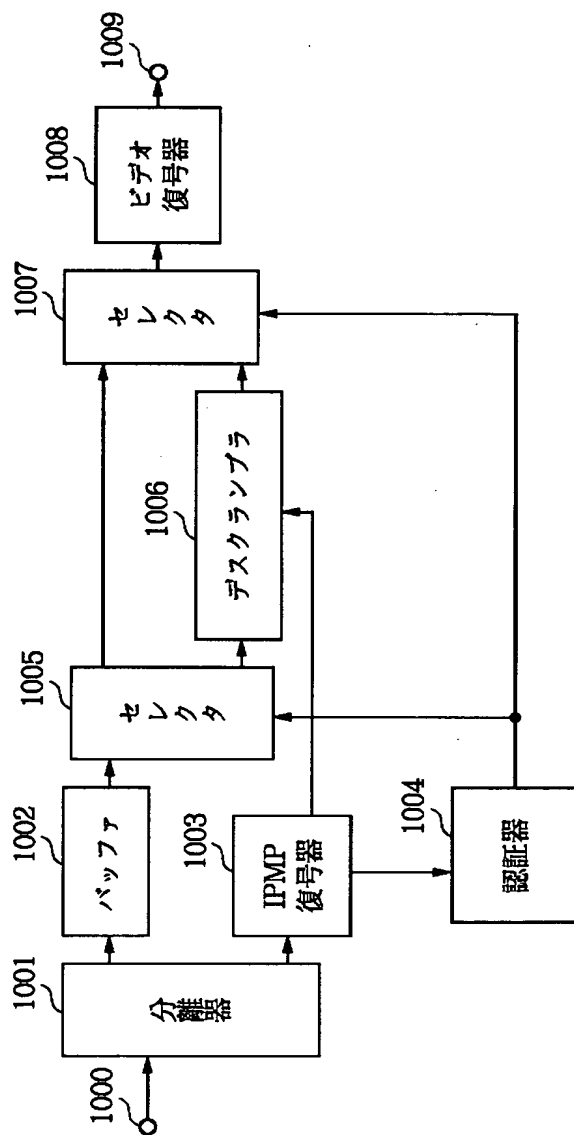
【図 8】



【図 9】

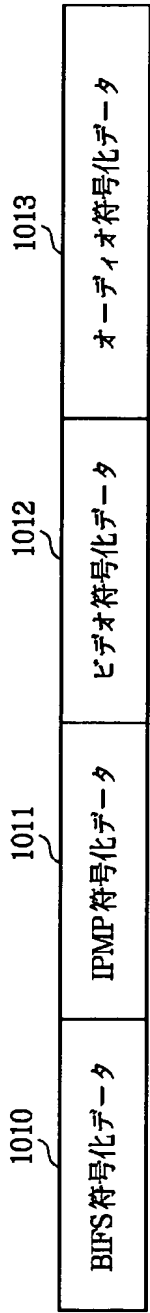


【図10】





【図 1 1】



【図 1 2】

IPMP 対象符号データ	ビデオ符号化データ
認証データ	nonac
セキュリティ対象	Frame No. 1～100      解読キー yek
	Frame No. 1000～1260      解読キー adeam

【書類名】 要約書

【要約】

【課題】 冗長データの発生を抑えながら画像の著作権（知的財産）保護ができる画像処理を提供する。

【解決手段】 画像データを入力する入力端子 1 0 0 と、前記画像データを保護するためのセキュリティデータを生成するセキュリティ設定器 1 0 4 と、前記画像データを符号化し、符号化データを生成するビデオ符号化器 1 0 1 と、前記セキュリティデータに従ってセキュリティが設定される区間の符号化データから一意に決定される VOP スタートコードを抽出するスタートコード検出器 1 0 5 と、前記 VOP スタートコードに前記セキュリティデータを重畳する暗号重畳器 1 0 6 と、前記セキュリティが設定された区間において前記 VOP スタートコードを除いた前記符号化データにスクランブルを施すスクランブラ 1 0 7 と、暗号重畳器 1 0 6 によって処理されたスタートコードとスクランブラ 1 0 7 によって処理された符号化データとを出力する合成器 1 1 1 とを有する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都大田区下丸子3丁目30番2号  
氏 名 キヤノン株式会社